

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 1. (Currently Amended) A state-varying hybrid stream cipher operating within a
2 computing device, comprising:

3 a first software routine to divide incoming plain text into variable-sized blocks with each
4 block varying in size in response to variations of an internal state of the computing device, the
5 internal state of the computing device being altered by the incoming plain text; and

6 a second software routine to convert the plain text into cipher text based on an encryption
7 key, an internal identifier and anthe internal state of the computing device.

1 2. (Currently Amended) The state-varying hybrid stream cipher of claim 1, wherein
2 the first software routine produces the variable-sized blocks based on the encryption key, the
3 internal identifier, andan output of a first non-linear function and the internal state of the
4 computer device.

1 3. (Original) The state-varying hybrid cipher of claim 2, wherein each current block
2 of the plain text is determined by (i) producing a pseudo-random sequence using a second non-
3 linear function including the encryption key, the internal identifier and the output of the first non-
4 linear function as inputs and (ii) accessing contents of the pseudo-random sequence as a number
5 of data elements of the plain text forming the current block.

1 4. (Original) The state-varying hybrid cipher of claim 1 further comprising:
2 a third software routine to determine if a plurality of random data elements are to be
3 distributed within the cipher text and to compute a hash digest of the random data elements.

1 5. (Original) The state-varying hybrid cipher of claim 4 further comprising a fourth
2 software routine to perform a first shuffling operation on the internal state of the computing

3 device based on the encryption key so that a single bit modification of the encryption key
4 requires complete recalculation of the internal state of the computing device used to encrypt the
5 random data elements.

1 6. (Currently Amended) The state-varying hybrid cipher of claim 4, wherein the
2 second software routine further performs a second shuffling operation on the internal state of the
3 computing device prior to encrypting the distribution of random data elements based on the
4 encryption key and the internal identifier to mitigate a likelihood of prediction of the internal
5 state of the computing device upon knowledge of the encryption key.

1 7. (Original) The state-varying hybrid cipher of claim 4, wherein the third software
2 routine determines a statistical amount of random data elements distributed within the cipher text
3 is programmable based on a percentage value entered by a user.

1 8. (Original) The state varying hybrid cipher of claim 7, wherein the distribution of
2 random data elements within the cipher text is based on the encryption key, the internal identifier
3 and internal state of the computing device.

1 9. (Original) The state-varying hybrid cipher of claim 1 further comprising a third
2 software routine to distribute error correcting codes in the cipher text in order to correct
3 modifications.

1 10. (Currently Amended) The state-varying hybrid cipher of claim 1, wherein the
2 internal state of the computing device is periodically modified without user intervention.

1 11. (Currently Amended) The state-varying hybrid cipher of claim 1, wherein the
2 internal state of the computing device is initialized by an Initialization Vector being a seed
3 valuebased on a time value.

1 12. (Currently Amended) A computing device comprising:
2 a memory; and

3 logic coupled to the memory, the logic to perform a state-varying stream cipher
4 operation, controlled by at least an encryption key and an internal state of the computing device,
5 on input data segmented in random sized blocks using the encryption key, the logic using an
6 initialization vector being a seed value only during an encryption process with no corresponding
7 seed value being used during a decryption process.

1 13. (Original) The computing device of claim 12, wherein the stream cipher
2 operation involves encryption.

1 14. (Original) The computing device of claim 12, wherein the logic is an integrated
2 circuit.

1 15. (Currently Amended) The computing device of claim 12, wherein the internal
2 state of the computing device varies over time without user intervention.

1 16. (Original) The computing device of claim 15, wherein the variation of the
2 internal state of the computing device is periodic being set at a time that an encryption process
3 begins for each block of input data.

1 17. (Currently Amended) The computing device of claim 12, wherein the computing
2 device is one of a smart card and an operating system.

1 18. (Currently Amended) The computing device of claim 12, wherein the logic of the
2 computing device segmenting segments the input data into at least three random sized blocks
3 with each block varying in length in response to variations of the internal state of the computing
4 device altered by the incoming plain text.

1 19. (Currently Amended) A method for decrypting input data using a combination of
2 stream cipher and block cipher functionality, comprising:
3 receiving as input a cipher text formed using an initialization vector operating as a seed
4 value, a decryption key, a percentage of random data and a unique internal identifier; and

5 reiteratively decrypting blocks of the cipher text without use of the initialization vector
6 and using the decryption key, the percentage of random data, the unique internal identifier and
7 a varying internal state of the computing device to recover corresponding blocks of plain text.

1 20. (Currently Amended) The method of claim 19, wherein the internal state of the
2 computing device varies ~~ever~~-continuously over time.